

**Abstract of JP 2000-29799**

**Problem to be solved:** To prevent the propagation of viruses from a transmitter side to the outside and to eliminate the time and labor of checking the viruses on a reception side.

**Solution:** At transmitting and receiving of electronic mail which utilize a network, a transmission side equipment checks whether or not the electronic mail to be transmitted is infected with the virus, transmits the fact that the virus is not detected, the name of a virus check software, and the proof of a version to the electronic mail in a form which is alteration impossible and transmits it. A reception side equipment verifies the proof and receives the electronic mail, when it is proper.

(19) 日本国特許庁 (J P)

## (12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2000-29799  
(P2000-29799A)

(43) 公開日 平成12年1月28日 (2000.1.28)

(51) IntCl.	識別記号	F I	テマコード(参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 G 5 B 0 8 9
H 0 4 L 12/54		H 0 4 L 11/20	1 0 1 B 5 K 0 3 0
12/58			

審査請求 未請求 請求項の数 8 O L (全 11 頁)

(21) 出願番号 特願平10-200443

(22) 出願日 平成10年7月15日 (1998.7.15)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 吉野 弘市郎

神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内

(74) 代理人 100078134

弁理士 武 順次郎

Fターム(参考) 5B089 AA21 AA22 AC05 AD11 AF05

CB02 CB03 DD07 EA08

5K030 GA12 GA15 HA06 LA01 LA07

LE12

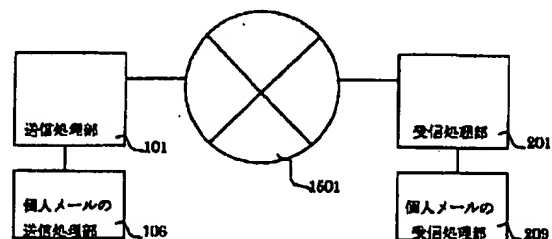
(54) 【発明の名称】 電子メールシステムの送信制御方法、受信制御方法及び電子メールシステム

(57) 【要約】

【課題】 送信者側から外部へのウイルスの拡散を防止すると共に、受信側でウイルスチェックをする手間を省くことを可能にする。

【解決手段】 ネットワークを利用した電子メールの送受信時に、送信側装置が、送信する電子メールにウイルスが感染しているか否かをチェックし、ウイルスが検出されないこと、ウイルスチェックソフトウェアの名前、バージョンの証明を改竄不可能な形で電子メールに付与して送信し、受信側装置が、前述の証明を検証し、正当であるときに電子メールを受信するようにする。

【図1】



【特許請求の範囲】

【請求項1】 ネットワークを介して電子情報を送受信する電子メールシステムの送信制御方法において、送信すべき電子情報の中にコンピュータウイルスが含まれているか否かをウイルスチェックソフトウェアにより検証し、検証の結果、コンピュータウイルスが検出されない場合にのみ、前記電子情報を送信することを特徴とする電子メールシステムの送信制御方法。

【請求項2】 前記検証の結果、コンピュータウイルスが検出されず、前記電子情報を送信するとき、コンピュータウイルスが検出されないという証明情報を前記送信すべき電子情報に付与することを特徴とする請求項1記載の電子メールシステムの送信制御方法。

【請求項3】 前記証明情報は、暗号化された情報であることを特徴とする請求項2記載の電子メールシステムの送信制御方法。

【請求項4】 前記検証の結果、コンピュータウイルスが検出されず、前記電子情報を送信するとき、コンピュータウイルスが検出されないという証明情報と、コンピュータウイルスが検出されないと検証したウイルスチェックソフトウェアの名称及びそのバージョン情報等の属性情報とを前記送信すべき電子情報に付与することを特徴とする請求項1記載の電子メールシステムの送信制御方法。

【請求項5】 ネットワークを介して電子情報を送受信する電子メールシステムの受信制御方法において、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されているか否かを認識し、受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合にのみ、前記電子情報を受信することを特徴とする電子メールシステムの受信制御方法。

【請求項6】 受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合、さらに、前記電子情報に付与されている証明を行ったウイルスチェックソフトウェアの名称、バージョン等の属性情報が妥当なものである場合に、電子情報を受信することを特徴とする請求項4記載の電子メールシステムの受信制御方法。

【請求項7】 ネットワークを介して電子情報を送受信する電子メールシステムの受信制御方法において、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されていない場合、あるいは、前記証明情報が付与されていても、前記電子情報に付与されている証明を行ったウイルスチェックソフトウェアの名称、バージョン等の属性情報が妥当なものでない場合に、前記電子情報を、前記電子情報の送信者に返送することを特徴とする電子メールシステムの受信制御方法。

【請求項8】 ネットワークを介して電子情報を送受信

する電子メールシステムにおいて、送信すべき電子情報の中にコンピュータウイルスが含まれているか否かをウイルスチェックソフトウェアにより検証する手段と、検証の結果、コンピュータウイルスが検出されない場合にのみ、前記電子情報に、コンピュータウイルスが検出されないという証明情報を付与して前記電子情報を送信する手段と、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されているか否かを認識する手段と、受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合にのみ、前記電子情報を受信する手段とを備えることを特徴とする電子メールシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、電子メールシステムの送信制御方法、受信制御方法及び電子メールシステムに係り、特に、送信者側から外部へのコンピュータウイルス（以下、単にウイルスという）の拡散を防止することができると共に、受信側でウイルスチェックをする手間を省くことができる電子メールシステムの送信制御方法、受信制御方法及び電子メールシステムに関する。

【0002】

【従来の技術】ウイルスの存在をチェックする方法に関する従来技術として、例えば、特開平7-146788号公報等に記載された技術が知られている。この従来技術は、計算機のOSまたはプログラムとして実行されるオブジェクトプログラム自身がウイルスへの感染を診断するというものである。また、他の従来技術として、送信する電子メールに対して、手作業によりウイルスチェックソフトウェアを用いてウイルスチェックを実施し、その結果を、例えば、「ABCウイルスチェック、バージョン1.0によりウイルスチェック実施済み。ウイルスはいません。」等の情報をその電子メールに書き込んで送信するものが知られている。

【0003】

【発明が解決しようとする課題】前述した従来技術は、電子メールの送信時に、自動的に電子メールに対するウイルスチェックを行うことについての配慮がなされておらず、ウイルスチェック漏れがあった場合、ネットワークを通してウイルスが拡散される恐れがあるという問題点を有している。

【0004】また、前述の従来技術は、電子メールの受信側装置において、送信側装置でのウイルスチェックの結果を自動的に判別して、受信メールの受理の可否を決定することについての配慮がなされていない。このため、前述の従来技術は、送信側において、手作業により付与されたウイルスチェックの結果について、それが受理できる範囲、例えば、ウイルスチェックを実施したウイルスチェックソフトウェアの製品名、バージョンが妥

当なものであるか否かについて人間の目で確認しなければならず、そのための作業が面倒であるという問題点を有している。

【0005】本発明の目的は、前述した従来技術の問題点を解決し、電子メールの送信時に自動的にウイルスチェックを実施し、その結果の情報とウイルスチェックをしたソフトウェアの情報とを電子メールに付与して送信する電子メールシステムの送信制御方法を提供することにある。

【0006】また、本発明の目的は、前述のようして送信された電子メールを受信する際に、受信側で受理可能なウイルスチェックソフトウェアの製品名、バージョン、ウイルスが検出されないことの証明がある電子メールのみを受理し、受理できない場合、その理由をつけて送信されてきた電子メールを送信側に返すようにした電子メールシステムの受信制御方法を提供することにある。

【0007】さらに、本発明の目的は、前述の送信と受信とを一体化した電子メールシステムを提供することにある。

【0008】

【課題を解決するための手段】本発明によれば前記目的は、ネットワークを介して電子情報を送受信する電子メールシステムの送信制御方法において、送信すべき電子情報の中にコンピュータウイルスが含まれているか否かをウイルスチェックソフトウェアにより検証し、検証の結果、コンピュータウイルスが検出されない場合のみ、前記電子情報を送信することにより、また、前記検証の結果、コンピュータウイルスが検出されず、前記電子情報を送信するとき、コンピュータウイルスが検出されないという証明情報を前記送信すべき電子情報に付与することにより、さらにまた、前記検証の結果、コンピュータウイルスが検出されず、前記電子情報を送信するとき、コンピュータウイルスが検出されないという証明情報と、コンピュータウイルスが検出されないと検証したウイルスチェックソフトウェアの名称及びそのバージョン情報等の属性情報とを前記送信すべき電子情報に付与することにより達成される。

【0009】さらに、前記目的は、前記証明情報に、ネットワーク上で改竄を受けることを避けるために、送信側あるいは受信側で確認可能な暗号化を施し、これにより、証明情報を信頼性の高い情報として送付することにより達成される。

【0010】また、前記目的は、ネットワークを介して電子情報を送受信する電子メールシステムの受信制御方法において、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されているか否かを認識し、受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合のみ、前記電子情報を受

信することにより、また、受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合、さらに、前記電子情報に付与されている証明を行ったウイルスチェックソフトウェアの名称、バージョン等の属性情報が妥当なものである場合に、電子情報を受信することにより達成される。

【0011】また、前記目的は、ネットワークを介して電子情報を送受信する電子メールシステムの受信制御方法において、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されていない場合、あるいは、前記証明情報が付与されていても、前記電子情報に付与されている証明を行ったウイルスチェックソフトウェアの名称、バージョン等の属性情報が妥当なものでない場合に、前記電子情報を、前記電子情報の送信者に返送することにより達成される。

【0012】さらに、前記目的は、ネットワークを介して電子情報を送受信する電子メールシステムにおいて、送信すべき電子情報の中にコンピュータウイルスが含まれているか否かをウイルスチェックソフトウェアにより検証する手段と、検証の結果、コンピュータウイルスが検出されない場合のみ、前記電子情報に、コンピュータウイルスが検出されないという証明情報を付与して前記電子情報を送信する手段と、受信しようとする電子情報に、コンピュータウイルスが検出されていないという証明情報が付与されているか否かを認識する手段と、受信しようとする前記電子情報にコンピュータウイルスが検出されていないという証明情報が付与されている場合のみ、前記電子情報を受信する手段とを備えることにより達成される。

【0013】さらに、前記目的は、受信しようとする前記証明情報が暗号化されている場合、受信側で暗号化された証明情報を確認して、例えば、暗号化された証明情報を解読する鍵を受信側が有しており、証明情報の解読が可能であることを確認して、そのときに電子メールを受け取るようにすることにより達成される。

【0014】

【発明の実施の形態】以下、本発明による電子メールの送受信制御方法及び電子メールシステムの実施形態を図面により詳細に説明する。

【0015】図1はネットワークを介して電子メールを送受信する本発明の一実施形態による電子メールシステムの構成を示すブロック図、図2は送信側の装置構成を示すブロック図、図3は受信側の装置構成を示すブロック図である。図1～図3において、101は送信処理部、102は送信指示受取部、103は証明情報付与部、104は送信判別部、105は送信部、106は個人メールの送信処理部、107はメール編集部、108はメール送信指示部、109はウイルスチェック部、201は受信処理部、202は受信部、203は付与情報読取部、204は配信判別部、205は拒絶通知編集部、2

06は拒絶メール送信部、207は拒絶情報通知部、208はメール配信部、209は個人メールの受信処理部、210は配信メール受取部、211は拒絶情報受取部、1501はネットワークである。

【0016】本発明の一実施形態による電子メールシステムは、図1に示すように、個人メールの送信処理部106が接続された送信処理部101と、個人メールの受信処理部209が接続された受信処理部201と、これらの送信処理部101及び受信処理部201の間を相互に接続するネットワーク1501とにより構成されている。送信処理部101及び受信処理部201は、通常、メールサーバの中に構成されていてよく、また、個人メールの送信処理部106、個人メールの受信処理部209は、個人ユーザのパソコン等の中に構成されていてよい。

【0017】前述のように構成される電子メールシステムにおいて、個人メールの送信処理部106から送信しようとする電子メールは、送信処理部101の判別により、ネットワーク1501を介して、受信処理部201に送信される。受信処理部201は、受信した電子メールの判別を行い、その結果により個人メールの受信処理部209に受信した電子メールを配信する。これらの処理については、図4、図5により後述する。

【0018】なお、前述では、個人メールの送信処理部106と個人メールの受信処理部209とが相互に電子メールの送受信を行うものとして、それぞれを別個の構成として示しているが、本発明は、個人メールの送信処理部106と個人メールの受信処理部209とを一体に構成してもよく、また、送信処理部101と受信処理部201とを1つのメールサーバ等の中に構成してもよい。

【0019】次に、送信処理部101及び個人メールの送信処理部106の構成を図2を参照して説明する。

【0020】送信処理部101は、通常、発信側のメールサーバの中に構成されており、図2に示すように、送信指示受取部102と、ウイルスチェック部109と、証明情報付与部103と、送信判別部104と、送信部105とにより構成される。また、個人メールの送信処理部106は、メール編集部107と、送信指示部108とにより構成される。

【0021】前述において、個人メールの送信処理部106のメール編集部107は、送信しようとするメールを編集するものであり、メール本文を作成し、宛て先の記入、選択、あるいは、メール本文に添付ファイルを添付する等の処理を行う。送信指示部108は、メール編集部107で編集されたメールを送信するように、送信処理部101に指示する。

【0022】送信処理部101の送信指示受取部102は、個人メールの送信処理部106の送信指示部108で送信指示されたメール及びその送信指示要求を受取

る。ウイルスチェック部109は、送信指示受取部102で送信指示されたメールに対してウイルスチェックを実施する。証明情報付与部103は、ウイルスチェック部109でのウイルスチェックの結果、ウイルスが検出されない場合に、ウイルスが検出されないことの証明情報と、ウイルスチェックをしたウイルスチェックソフトウェアの名前、及び、そのバージョン等の属性情報とを前記メールに付与する。

【0023】なお、前述で送信するメールに付与する情報は、ネットワーク上での改竄を防止するために暗号化された情報で、ウイルスチェック部109及び情報付与部103が、メールに付与するものであり、オペレータがキーボード等からその情報を入力するものではない。

【0024】次に、受信処理部201及び個人メールの受信処理部209の構成を図3を参照して説明する。

【0025】受信処理部201は、通常、受信側のメールサーバの中に構成されており、図3に示すように、受信部202と、付与情報読取部203と、配信判別部204と、拒絶通知編集部205と、拒絶メール送信部206と、拒絶情報通知部207と、メール配信部208とにより構成される。また、個人メールの受信処理部209は、配信メール受取部210と、拒絶情報受取部211とにより構成される。

【0026】前述において、受信処理部201の受信部202は、メールを受信するものであり、付与情報読取部203は、受信部202で受信された電子メールに暗号化された情報として付与されているウイルスが検出されないことの証明情報と、ウイルスチェックをしたウイルスチェックソフトウェアの名前及びバージョン等の情報とを読み取る。

【0027】また、受信部202で受信された電子メールに暗号化された情報が付与されている場合、受信部202は、受信部202が管理している暗号鍵で暗号化された情報を解読し、解読できない場合、その電子メールの受信側での配信を行わないように配信判別部204に指示する。

【0028】配信判別部204は、付与情報読取部203で読み取った情報から、前記メールを前記メールに記載の宛て先に配信するか否かを判別するものであり、例えば、ウイルスが検出されないことの証明情報が無い場合、前記の宛て先にメールを配信しないと判別する。また、配信判別部204は、例えば、ウイルスチェックを実施したウイルスチェックソフトウェアの名前が受信側で認めていないものであったり、バージョンが古い場合、前記の宛て先にメールを配信しないと判別する。そして、配信判別部204は、ウイルスが検出されないことの証明情報を読み取り、さらに、ウイルスチェックソフトウェアの名前やバージョンが受信側で許可できるものであれば、前記の宛て先にそのメールを配信すると判別する。

【0029】拒絶通知編集部205は、配信判別部204が宛先に配信しないと判別したメールについて、配信しないと理由情報を作成するもので、例えば、ウイルスチェックをした証明の情報がないから配信しない、ウイルスチェックをしたウイルスチェックソフトウェアが受信側で認めていないものであるという理由の情報を作成する。拒絶メール送信部206は、拒絶通知編集部205が作成した理由情報をそのメールに付与して、メールの送信者に送り返すものである。拒絶情報通知部207は、拒絶通知編集部205で作成した理由情報を、そのメールの宛て先に通知するものである。メール配信部208は、配信判別部204が配信すると判別したメールをそのメールの宛て先に配信する。

【0030】個人メールの受信処理部209は、メールの宛て先となるものであり、受信処理部201のメール配信部208から配信されるメールを配信メール受取部210で受信し、また、拒絶情報通知部207から通知される拒絶の理由情報を拒絶情報受取部211で受信する。

【0031】図4は図2に示す送信処理部によるメールの送信制御の処理動作を説明するフローチャートであり、以下、これについて説明する。

【0032】(1)個人メールの送信処理部106において、送信者がメールを編集しそのメールを送信処理部101に送り、メールの送信指示を行うと、送信処理部101は、送信が指示されたメール本文及びメールに添付されるファイルがウイルスに感染していないか否かのウイルスチェックを行う(ステップ301、302)。

【0033】(2)そして、ウイルスチェックの結果、ウイルスが検出されたか否かが判別される(ステップ303)。

【0034】(3)ステップ303のチェックの結果、ウイルスが検出されない場合、ウイルスが検出されないことの証明情報と、ウイルスチェックをしたウイルスチェックソフトウェアの名前及びバージョン等の属性情報とを改竄困難な形でそのメールに付与する(ステップ304、306)。

【0035】(4)ステップ306の処理終了後、ステップ301でメールの送信指示で指定された送信先にそのメールを送信する(ステップ307)。

【0036】(5)ステップ303のチェックの結果、ウイルスが検出されていた場合、そのメールの送信先への送信を行わず、ウイルスの存在を送信者の画面等に表示する等のために送信者である個人メールの送信処理部106に知らせる(ステップ305、308)。

【0037】図5は図3に示す受信処理部によるメールの受信制御の処理動作を説明するフローチャートであり、以下、これについて説明する。

【0038】(1)ネットワークを介してメールが受信されると、受信処理部201において、メールに付与さ

れているウイルスが検出されないことの証明情報と、ウイルスチェックをしたウイルスチェックソフトウェアの名前、及び、そのバージョン等の属性情報とが読み込まれる(ステップ401、402)。

【0039】(2)そして、これらの読み込んだ情報から受信したメールの受理の可否を判別する。この判別は、ウイルスが検出されないことの証明があるか否か、ウイルスチェックをしたウイルスチェックソフトウェアの名前とそのバージョン等の属性情報とが、受信側で予め設定した幾つかのウイルスチェックソフトウェアの名前とそのバージョンと一致するか否かにより行われる(ステップ403)。

【0040】(5)ステップ403の判別で、ウイルスが検出されない証明があり、かつ、ウイルスチェックをしたウイルスチェックソフトウェアの名前とバージョン等の属性情報が、受信側で予め設定した幾つかのウイルスチェックソフトウェアの名前とそのバージョン等の属性情報とに一致している場合、そのメールの受理が可能と判別され、そのメールをメールに記載されている宛て先に配信する(ステップ404、406)。

【0041】(6)また、ステップ403の判別で、ウイルスが検出されない証明がない場合、あるいは、ウイルスチェックをしたウイルスチェックソフトウェアの名前とバージョンとの情報が、受信側で予め設定した幾つかのウイルスチェックソフトウェアの名前とそのバージョンとに一致していない場合、そのメールの受理が不可能と判別される(ステップ405)。

【0042】(7)受理不可能と判別された場合、受理不可能とした拒絶通知の編集が行われ、「受理不可能だから、送信者に送り返しました。」等の不信通知の編集が行われる。そして、そのメールを拒絶メールとして送信者へ送り返し、さらに、そのメールに記載の宛て先に、メールを配信しなかったことを通知する。拒絶通知は、例えば、ウイルスが検出されないという情報がないから受理不可という拒絶通知、あるいは、ウイルスチェックソフトウェアの名前やバージョンが受信側で予め設定した幾つかのウイルスチェックソフトウェアの名前とそのバージョンに適合しないから受理不可という拒絶通知である(ステップ407、409、408)。

【0043】図6はメールのデータ構造を説明する図、図7は拒絶メールのデータ構造を説明する図、図8は不信通知メールのデータ構造を説明する図であり、以下、これらについて説明する。

【0044】前述したステップ307のメールの送信処理で送信されるメールのデータは、図6に示すように、宛て先情報501と、送信者情報502と、メールのタイトル情報503と、メール本文の情報504と、メールに添付するファイルの情報505と、ウイルスチェック証明情報506と、その他情報507とにより構成される。宛て先情報501は、メールの宛て先の名前、ア

ドレス等の情報であり、送信者情報502は、メールの送信者の名前、アドレス等の情報である。メールのタイトル情報503は、送信するメールの題名、タイトルである。メール本文の情報504は、送信するメールの本文の情報である。メールに添付するファイルの情報505は、送信するメールに添付するファイルの情報である。ウイルスチェック証明情報506は、送信するメールにウイルスが検出されないという証明と、ウイルスが検出されなかった、ウイルスチェックソフトウェアの名前、そのバージョン、日付等の情報である。その他の情報507は、メールが至急であるとか、返信が必要とか、受信確認をしたり、また、他のメールを送信するための制御情報等である。

【0045】前述したステップ408の拒絶通知、不信通知の送信処理で、メールの送信者に送り返す拒絶メールのデータは、図7に示すように、送信者情報502と、メールサーバの情報601と、メールのタイトル情報503と、メール本文の情報504と、メールに添付するファイルの情報505と、拒絶通知情報602とにより構成される。メールサーバの情報601は、メールを受信したメールサーバの名前、アドレス等の情報であり、拒絶通知情報602は、ステップ407の拒絶通知編集処理で編集された拒絶通知である。その他の情報は、図6の場合と同一である。なお、拒絶通知情報602については後述する。

【0046】前述したステップ408の拒絶通知、不信通知の送信処理で、メールの宛て先に当該のメールを配信しないと通知する不信通知メールのデータは、図8に示すように、宛て先情報501と、メールサーバの情報601と、送信者の情報502と、メールのタイトル情報503と、不信通知情報701とにより構成される。不信通知情報701は、ステップ409の不信通知の編集処理で編集されたそのメールを配信しなかったことの通知であり、他の情報は、図6、図7の場合と同一である。なお、不信通知情報701については後述する。

【0047】次に、前述した本発明の一実施形態による各種の処理時に、メールの送信者、受信者に表示される画面例を説明する。

【0048】図9は送信者がメールを送信しようとするときのメールの送信画面例を示す図である。

【0049】メール送信画面801は、送信タイトル802と、宛て先803と、メール本文804と、添付ファイル805と、送信アイコン806と、状態表示807とにより成る。送信タイトル802は、送信メールのタイトルであり、図示例では「特許取得しました」というタイトルである。宛て先803は、メールの宛て先であり、「東京太郎」へ送信するメールを示している。メール本文804は、メールの本文である。添付ファイル805は、メールに添付する幾つかの添付ファイルである。送信アイコン806は、メール本文804と、添付

ファイル805を送信しようとする場合に使用するアイコンである。送信アイコン806を選択すると、メール本文804と、添付ファイル805とに対してウイルスチェックが開始され、ウイルスチェック中であることが状態表示807に表示される。図示の例では、状態表示807には、「ウイルスチェック中」との状態が表示されている。

【0050】図10はウイルスチェックをした結果、ウイルスが検出されないときのメールの送信者に対する表示画面例を示す図である。

【0051】ウイルスが検出されないときの表示画面901は、タイトル802と、宛て先803と、メール本文804と、添付ファイル805と、送信完了の情報表示902とにより成る。なお、802～805は、図9の場合と同一である。

【0052】送信完了の情報表示902は、ウイルスチェックの結果、ウイルスが検出されないことを表示するものである。図示例では、送信完了の情報表示902には、ウイルスチェックの結果、ウイルスが検出されないこと、そのウイルスチェックを実施したウイルスチェックソフトウェア名及びそのバージョン情報、及び、ウイルスチェック終了時刻が表示されている。

【0053】図11はウイルスチェックをした結果、ウイルスが存在するときのメールの送信者に対する表示画面例を示す図である。

【0054】ウイルスが存在するときの画面1001は、タイトル802と、宛て先803と、メール本文804と、添付ファイル805と、送信却下の情報表示1002とにより成る。なお、802～805は図9の場合と同一である。

【0055】送信却下の情報表示1002は、ウイルスチェックの結果、ウイルスがいたことを表示するものである。図示例では、送信却下の情報表示1002には、ウイルスチェックの結果、ウイルスがいたことと、その場所と、ウイルスチェックを実施したウイルスチェックソフトウェア名と、そのバージョン情報と、ウイルスチェック終了時刻とが表示されている。このとき、警告のために、ウイルスが存在するときの画面1001の背景を赤色等で表示したり、点滅したりさせることもできる。

【0056】図12はメールの受信者に対してメールの受信を知らせる表示画面例を示す図である。

【0057】メール受信表示画面1101は、受信メールの一覧1102と、全受信状況確認アイコン1103より成る。受信メールの一覧1102に表示されている受信メールは、ウイルスが検出されないという証明と、受信側で指定した名前とそのバージョンとに相当するウイルスチェックソフトウェアでのウイルスチェックが施されている証明があった受信メールである。そして、受信メールの一覧1102には、送信者1104と、受信

日付1105と、タイトル803とが認識できるように一覧表示されている。例えば、神奈川からきたメール1107の送信者は「神奈川一郎」、受信日付は「1999年8月10日」、タイトルは「特許取得しました」である。もし、ウイルスが検出されないという証明、受信側で指定した名前とそのバージョンとに相当するウイルスチェックソフトウェアでのウイルスチェックが施されたという証明がないとき、該当するメールは拒絶され、受信メールの一覧1102には表示されず、その情報は全受信状況確認アイコン1103を指定することにより確認することができる。

【0058】図13は図12に示す表示画面の全受信状況確認アイコン1103が選択されたときに表示される全受信状況表示画面を示す図である。

【0059】全受信状況表示画面1201は、全受信メールの一覧表示1202と、拒絶情報表示1206と、拒絶詳細アイコン1205とより成る。全受信メールの一覧表示1202には、受理状況1203と、送信者1104と、受信日付1105と、タイトル1106とが判るように全情報メールが表示される。図示例では、神奈川からきたメール1107と、横浜からきたメール1204とが表示されている。

【0060】受理状況1203は、受信メールを配信せずに、メールの送信者へ送り返したものについて表示するものであり、図示例では、横浜からきたメール1204が受理状況1203に相当する位置に「拒絶」と表示されている。これにより、受信者は、このメールが配信されず、メールの送信者へ送り返されたことが判る。詳細アイコン1205は、送り返したメールの情報を確認する場合に選択され、このアイコンが選択された場合、拒絶情報表示1206が表示される。拒絶情報表示1206には、送り返した横浜からきたメール1204について、メールサーバで受信した受信日と送信者とタイトルとが判るように表示され、また、送り返した理由として、メールのウイルスチェックを行ったウイルスチェックソフトウェアが受信側で認めないものである場合等に、そのことが表示がされる。図示例の場合、横浜からきたメール1204のウイルスチェックを行ったウイルスチェックソフトウェアが、受信側のAAメールサーバで認めていないZZチェックであることが判る。さらに、このメールについて、受信者は、その内容を見ることができず、送信者11104と受信日付1105とタイトル1106とが判るだけである。

【0061】図14は送信者がメール送信処理を行った後、そのメールが宛て先に届いたか否かを確認するための受信状況を表示する送信者の表示画面例を示す図である。

【0062】受信状況を表示する送信者への表示画面1301は、送信者が前述したステップ307のメールの送信処理を行った後に表示され、送信メール一覧130

2と、拒絶状況詳細アイコン1309と、拒絶理由詳細表示1310とよりなる。この表示画面1301において、送信メール一覧1302に表示されるメールのそれぞれは、受信状況1303と、宛て先803と、送信日付1305と、タイトル802とが判るように表示されている。例えば、千葉宛のメール1307は、「こんにちうさまへ」というタイトルで、1999年8月1日に千葉三郎へ送信しており、既に開封されていることが表示される。また、東京宛のメール1308は、「ういるすあるぞう」というタイトルで、1999年9月11日に東京太郎へ送信しているが、このメールは拒絶され、送り返されてきたことが表示されている。

【0063】そして、この拒絶の理由は、拒絶状況詳細アイコン1309を選択することにより、拒絶理由詳細表示1310に表示される。拒絶理由詳細表示1310によると、1999年9月11日の該当メールの送信日付1311で、該当メールの宛て先1312のメールは、受信側のメールサーバ1314であるBBメールサーバにより拒絶されたことが判る。さらにその詳細は、拒絶通知アイコン1313を選択することにより、拒絶通知編集部205で編集された拒絶通知が表示される。

【0064】図15は図14に示す拒絶通知アイコン1313が選択されたときに表示される拒絶通知表示画面例を示す図である。

【0065】拒絶通知表示画面1401には、送信したメールが受信側のサーバで拒絶された理由が詳細に示されされる。この理由の詳細は、受信側のサーバにおける拒絶通知編集部205で編集されて返送されてきたものである。図示の拒絶通知表示画面1401によれば、1999年9月11日の送信日付1311で、東京太郎の宛て先1312に、「ういるすあるぞう」のタイトル1402で送信されたメールは、このメールのウイルスチェックを行ったウイルスチェックソフトウェアが、受信側のメールサーバで認可できるものでなかったために返却されたことが判る。そして、受信側のメールサーバで認可できるウイルスチェックソフトウェアの名称とそのバージョンとが表示される。

【0066】前述した本発明の一実施形態によれば、メールの送信時に自動的にウイルスチェックを実施し、ウイルスがない場合に限り、その結果の情報とウイルスチェックをしたソフトウェアの情報とを電子メールに付与して送信することが可能なため、ウイルスがメールにいた場合は送信不可とすることができる。このため、外部へのウイルスの拡散を避けることができる。

【0067】また、前述した本発明の一実施形態によれば、送信された電子メールを受信する際、受信側で受理可能なウイルスチェックソフトウェアの製品名やバージョンと、ウイルスが検出されないことの証がある電子メールのみを受理し、さらに、メールを受理することができない場合、その理由を付けて送信されてきた電子メー



ルを送信側に返すことができるため、受信側でウイルスチェックをする手間を省くことができる。

【0068】本発明の一実施形態によれば、前述により、ウイルスチェックをしていないものは受け取らないという姿勢をインターネット等の通信回線上に流行させることが可能となり、ウイルスの広がりを押さえる効果をも得ることができる。

【0069】

【発明の効果】以上説明したように本発明によれば、電子メールの送信時に自動的にウイルスチェックを実施し、その結果の情報とウイルスチェックをしたソフトウェアの情報とを電子メールに付与して送信する電子メールの送信制御方法、及び、前述のようにして送信された電子メールを受信する際に、受信側で受理可能なウイルスチェックソフトウェアの製品名、バージョン、ウイルスが検出されないことの証明がある電子メールのみを受理し、受理できない場合、その理由をつけて送信されてきた電子メールを送信側に返すようにした電子メールの受信制御方法を提供することができる。

【0070】本発明によれば、前述により、送信者側から外部へのウイルスの拡散を防止することができると共に、受信側でウイルスチェックをする手間を省くことができる。

【図面の簡単な説明】

【図1】ネットワークを介して電子メールを送受信する本発明の一実施形態による電子メールシステムの構成を示すブロック図である。

【図2】送信側の装置構成を示すブロック図である。

【図3】受信側の装置構成を示すブロック図である。

【図4】図2に示す送信処理部によるメールの送信制御の処理動作を説明するフローチャートである。

【図5】図3に示す受信処理部によるメールの受信制御の処理動作を説明するフローチャートである。

【図6】メールのデータ構造を説明する図である。

【図7】拒絶メールのデータ構造を説明する図である。

【図8】不信通知メールのデータ構造を説明する図である。

【図9】送信者がメールを送信しようとするときのメールの送信画面例を示す図である。

【図10】ウイルスチェックをした結果、ウイルスが検出されないときのメールの送信者に対する表示画面例を示す図である。

【図11】ウイルスチェックをした結果、ウイルスが存在するときのメールの送信者に対する表示画面例を示す図である。

【図12】メールの受信者に対してメールの受信を知らせる表示画面例を示す図である。

【図13】図12に示す表示画面の全受信状況確認アイコンが選択されたときに表示される全受信状況表示画面を示す図である。

【図14】送信者がメール送信処理を行った後、そのメールが宛て先に届いた否かを確認するための受信状況を表示する送信者の表示画面例を示す図である。

【図15】図14に示す拒絶通知アイコンが選択されたときに表示される拒絶通知表示画面例を示す図である。

【符号の説明】

- 101 送信処理部
- 102 送信指示受取部
- 103 証明情報付与部
- 104 送信判別部
- 105 送信部
- 106 個人メールの送信処理部
- 107 メール編集部
- 108 メール送信指示部
- 109 ウイルスチェック部
- 201 受信処理部
- 202 受信部
- 203 付与情報読取部
- 204 配信判別部
- 205 拒絶通知編集部
- 206 拒絶メール送信部
- 207 拒絶情報通知部
- 208 メール配信部
- 209 個人メールの受信処理部
- 210 配信メール受取部
- 211 拒絶情報受取部
- 1501 ネットワーク

【図6】

【図6】

宛て先 情報	送信者 情報	メールのタ イトル情報	メール本 文の情報	メールに添付する ファイルの情報	ウイルスチェ ック証明情報	その他 情報
501	502	503	504	505	506	507

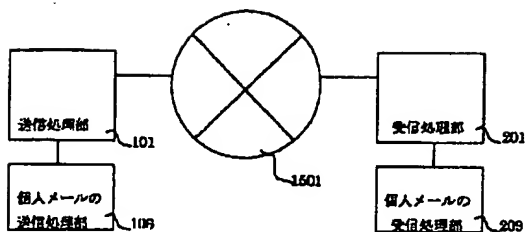
【図7】

【図7】

送信者 情報	メールサーバ の情報	メールのタ イトル情報	メール本 文の情報	メールに添付する ファイルの情報	拒絶通知 情報
502	601	503	504	505	502

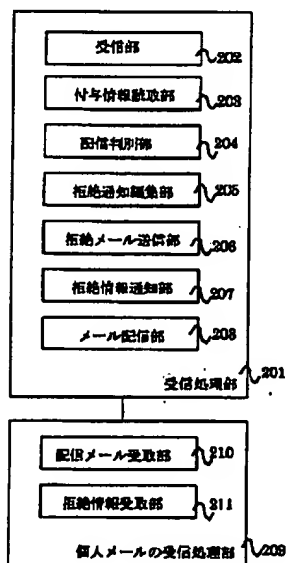
【図 1】

【図 1】



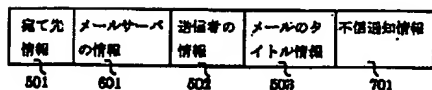
【図 3】

【図 3】



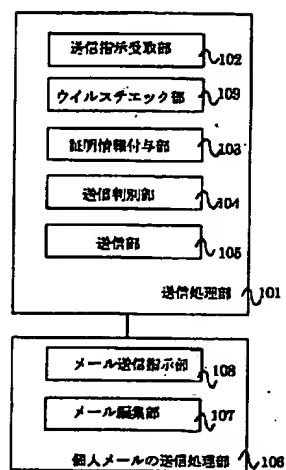
【図 8】

【図 6】



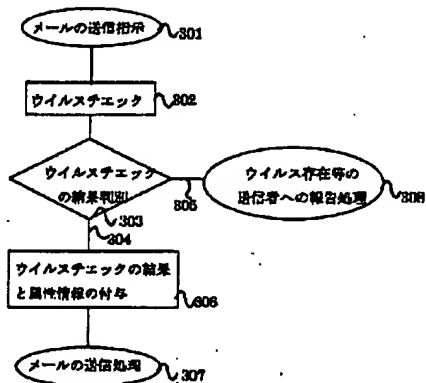
【図 2】

【図 2】



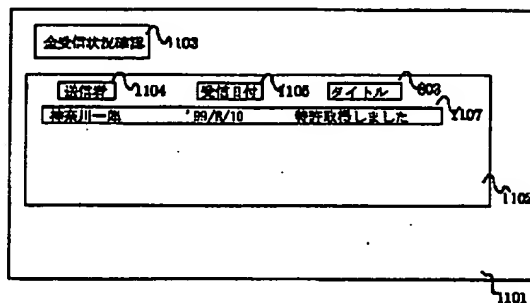
【図 4】

【図 4】



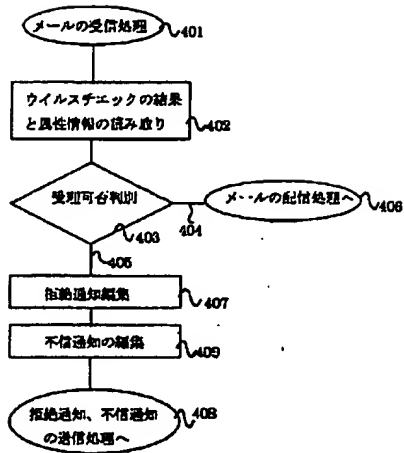
【図 1 2】

【図 1 2】



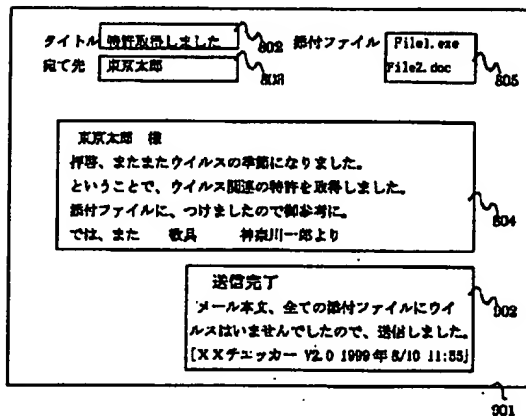
【図 5】

【図 5】



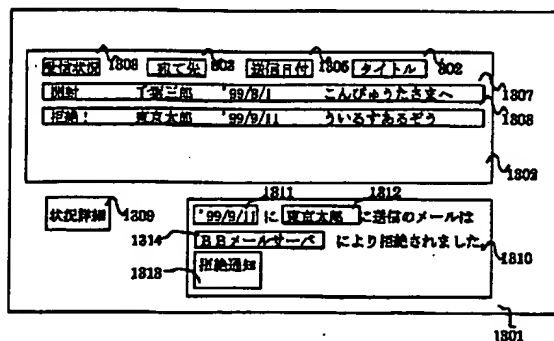
【図 10】

【図 10】



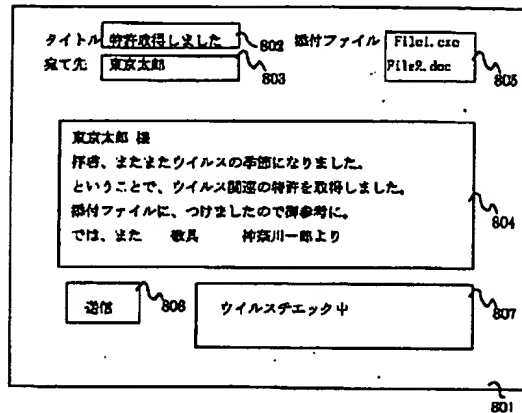
【図 14】

【図 14】



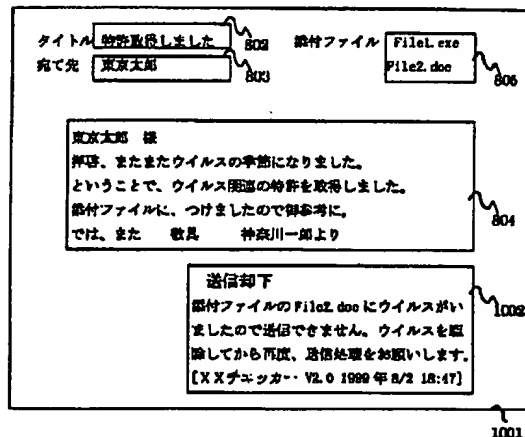
【図 9】

【図 9】



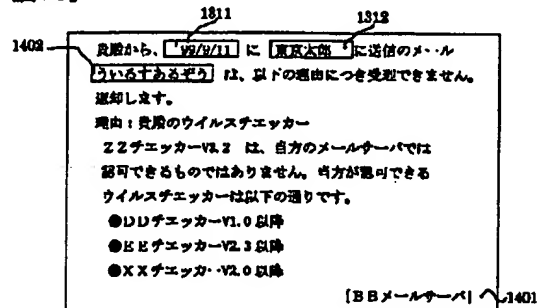
【図 11】

【図 11】



【図 15】

【図 15】



【図13】

【図13】

処理状況	送信者	受信日時	タイトル
	仲森川一郎	'99/9/10	特許取得しました
拒絶	横田三郎	'99/9/11	ういうすあるぞう

拒絶詳細

☆ '99/9/11 にきた 横田三郎 のメール『ういうすあるぞう』を拒絶しました。

☆理由: クイルスチエッカー  
 エスチエッカー を、自力では認めません。 [AAメールサーバ]

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**